



DEPARTMENT OF THE TREASURY

Internal Revenue Service

Privacy Act of 1974, as amended

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Notice of proposed modification to Privacy Act system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the Department of the Treasury, Internal Revenue Service, gives notice of proposed modifications to system of records entitled: Treasury/IRS 60.000 Employee Protection System Records.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The new and modified routine uses will be applicable on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This altered system of records will be effective October 1, 2020, unless the IRS receives comments that would result in a contrary determination.

ADDRESSES: Comments should be sent to the Office of Privacy, Governmental Liaison and Disclosure, Internal Revenue Service, 1111 Constitution Avenue NW, Washington, DC 20224. Members of the public desiring specific information concerning this notice may request information at the address provided above.

FOR FURTHER INFORMATION CONTACT: John J Walker, Associate Director, Incident Management & Employee Protection, IRS Office of Privacy, Governmental Liaison and Disclosure, (267) 466-2416 (not a toll-free number).

SUPPLEMENTARY INFORMATION: The proposed revisions will enable better awareness of potential risks and will increase safety and security for current and former IRS employees. The Potentially Dangerous Taxpayer (PDT) designation improves the Service's ability to identify individuals who represent a potential danger to employees, including individuals who have physically assaulted, threatened, or intimidated employees or are of members of groups that advocate violence against IRS employees or other federal employees. The Caution Upon Contact (CAU) designation is used when the threat is less severe, the taxpayer threatens suicide, or when the taxpayer files or threatens to file a frivolous lien or a frivolous criminal or civil legal action.

Continual program introspection and the current landscape for IRS staff having contact with the public, including self-radicalization, prompted the IRS to reevaluate the Office of Employee Protection (OEP) program and institute a higher level of protection for its employees. To accomplish this the IRS is planning to (1) add information about individuals who threaten former IRS employees related to their prior work performing official IRS duties, (2) add information about individuals who are advocating violence against U.S. Government employees in general or demonstrating violent tendencies against U.S. Government employees of other federal agencies, (3) remove the “active” qualifier, as it applies to membership in group(s) advocating violence, and (4) add a specific time-period during which the individual’s activity will be considered (within the past 10 years) to ensure an accurate, comprehensive, and complete analysis is completed before a potentially dangerous taxpayer (PDT) or caution upon contact (CAU) designation is assigned. The purpose statement is amended to reflect these revisions. Pursuant to Office of Management and Budget (OMB) Memorandum M-17-12, an additional routine use is added to ensure that IRS can assist another agency in responding to a confirmed or suspected breach, as appropriate. As required by the Privacy Act of 1974, 5 U.S.C. 552a(r), a report of altered system of records has been provided to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget. The proposed modifications to the system of records are published below.

Ryan Law,

Deputy Assistant Secretary for Privacy, Transparency, and Records.

SYSTEM NAME AND NUMBER:

Department of the Treasury, IRS 60.000 - Employee Protection System Records

SECURITY CLASSIFICATION:

Information contained in this system is unclassified.

SYSTEM LOCATION:

Records are maintained at the Internal Revenue Service Headquarters in Washington, D.C. and field and campus offices at the following addresses, 1111 Constitution Avenue NW., Washington, DC 20224; 500 Woodward Avenue, Detroit, MI 48226; and 2970 Market Street, Philadelphia, PA 19104.

SYSTEM MANAGER(S):

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 26 U.S.C. 7801.

PURPOSE(S) OF THE SYSTEM:

This system of records maintains records that reflect attempts or intention to obstruct or impede current or former IRS employees or contractors in the performance of their official duties, including records of investigations into the individual's actions and records of conclusions as to whether an individual should be considered potentially dangerous to any such employee, contractor, or their immediate family members, or should otherwise be approached with caution.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals attempting to interfere with the administration of internal revenue laws through assaults, threats, suicide threats, filing or threats of filing frivolous criminal or civil legal actions against Internal Revenue Service (IRS) employees, (current for former) or IRS contractors or the employees' or contractors' immediate family members, or through forcible interference against any officer, government contractor or employee while discharging the official duties at his/her position. An individual is designated as a PDT based on reliable information furnished to the IRS or Treasury Inspector General for Tax Administration (TIGTA), that fits any of the criteria (1) through (6) below: (1) Individuals who, within the past 10 years, have physically assaulted an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee or a contractor; (2) individuals who, within the past 10 years, have intimidated or threatened an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee, or a contractor through specific threats of bodily harm, a show of weapons, the use of animals, or through other specific threatening behavior (e.g., stalking, etc.); (3) Individuals who, within the past 10 years, have advocated violence against IRS employees where advocating such violence could reasonably be understood to threaten the safety of Service employees and/or impede the performance of Service duties; (4) Individuals who, within the past 10 years, have been members of, or affiliated with groups that advocate violence against IRS employees, where advocating such violence could reasonably be understood to threaten the safety of Service employees or impede the performance of Service duties; (5) Individuals who, within the past 10 years, have committed the acts set forth in any of the preceding criteria, but whose acts have

been directed against employees or contractors of other governmental agencies; (6) Individuals who are not classified as PDTs through application of the above criteria, but whose acts within the past 10 years have demonstrated a propensity for violence. An individual is designated as an individual who should be approached with caution (CAU) based on reliable information furnished to the IRS or the TIGTA that fits any of the criteria (1) through (3) below: 1) Individuals who, within the past 10 years, have threatened physical harm that is less severe or immediate than necessary to satisfy PDT criteria. 2) Individuals who, within the past 10 years, have threatened suicide, 3) Individuals who, within the past 10 years, have filed or threatened to file a frivolous lien or a frivolous civil or criminal legal action against an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee, or contractor.

PDT and CAU designations will be reviewed at or near every five years from the date of the initial or the last renewal of the designation to determine whether the circumstances leading to the designation, and any new relevant information about the individual's conduct, continue to indicate potential danger to IRS employees, former employees, contractors, or their family members. If these facts and circumstances continue to indicate potential danger, the designation will be renewed for, and subject to review after, an additional five years.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Individual's name;
- Business name;
- Date of birth;
- Date of death;
- Gender;
- Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or similar number assigned by the IRS);
- Centralized Authorization Files (CAF) numbers;
- Addresses;
- Documentary evidence of the incident (e.g. threatening correspondence, copies of liens and legal actions, and contact recording transcripts);

- Documentation of investigation of incident (report of investigation, statements, affidavits, and related tax information);
- Records of any legal action resulting from the incident;
- FBI or Police records of individual named in the incident;
- Newspaper or periodical items or information from other sources provided to the IRS or TIGTA for investigation of individuals who have demonstrated a clear propensity toward violence;
- Correspondence regarding the reporting of the incident, referrals for investigation, investigation of the incident; and result of investigation (i.e. designation as PDT or CAU).

RECORD SOURCE CATEGORIES:

Records are obtained from other IRS offices and the Treasury Inspector General for Tax Administration (TIGTA).

ROUTINE USES: OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USE:

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Material covered by rule 6(e) of the Federal Rules of Criminal Procedure may be disclosed only as permitted by that rule. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

(1) Disclose information to the Department of Justice (DOJ) when seeking legal advice, or for use in any proceeding, or in preparation for any proceeding, when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her individual capacity if the IRS or the DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by the proceeding, and the IRS determines that the records are relevant and useful.

(2) Disclose information in a proceeding (including discovery) before a court, administrative tribunal, or other adjudicative body when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her personal capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS or DOJ determines that the information is relevant and necessary to the

proceeding. Information may be disclosed to the adjudicative body to resolve issues of relevancy, necessity, or privilege pertaining to the information.

(3) Disclose information to a Federal, state, local, or tribal agency, or other public authority, which has requested information relevant or necessary to hiring or retaining an employee, or issuing or continuing a contract, security clearance, license, grant, or other benefit.

(4) Disclose information to an appropriate Federal, state, local, tribal, or foreign agency, or other public authority, responsible for implementing or enforcing, or for investigating or prosecuting the violation of, a statute, rule, regulation, order, or license, when a record on its face, or in conjunction with other records, indicates a potential violation of law or regulation and the information disclosed is relevant to any regulatory, enforcement, investigative, or prosecutorial responsibility of the receiving authority.

(5) Disclose information to the news media as described in the IRS Policy Statement P-1-183, News Coverage to Advance Deterrent Value of Enforcement Activities Encouraged, IRM 1.2.1.2.41.

(6) Disclose information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

(7) To appropriate agencies, entities, and persons when (1) the Department of the Treasury and/or Treasury bureau suspects or has confirmed that there has been a breach of the system of records; (2) the Department of the Treasury and/or Treasury bureau has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of the Treasury and/or Treasury bureau (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of the Treasury's and/or Treasury bureau's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(8) To another Federal agency or Federal entity, when the Department of the Treasury and/or Treasury bureau determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name or Social Security Number (SSN) of individual with respect to whom the PDT or CAU designation is being considered and by administrative case control number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are managed in accordance with National Archives and Records Administration (NARA) General Records Schedule 5.6 item 170 & 171.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances.

RECORD ACCESS PROCEDURES:

See “Notification Procedures” below.

CONTESTING RECORD PROCEDURES:

See “Notification Procedures” below.

NOTIFICATION PROCEDURES:

The Secretary of Treasury has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, Treasury, IRS will consider individual requests to determine whether information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendices A-M. Requests for information and requests for records should be marked “Privacy Act Request” on the outside and mailed to the following address: Internal Revenue Service, Disclosure Scanning Operation—Stop 93A, Post Office Box 621506, Atlanta, GA 30362-3006.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 31 CFR 1.36. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. No specific form is required. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which bureau(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the Bureau or Freedom Of Information Act staff determine which Treasury Bureau may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the Bureau(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Department of the Treasury has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1), (e)(4)(G)-(I) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). (See 31 CFR 1.36.).

HISTORY:

Notice of this system of records was last published in full in the Federal Register on Sept. 8, 2015 (80 FR 54063) as the Department of the Treasury, IRS 60.000 - Employee Protection System Records.